

REMARKS

The Examiner rejected claims 29-46 and 51-52 under §103(a) as being obvious over Pasieka in view of Schneier (“Applied Cryptography”). Applicants disagree.

The claimed invention is directed to a two-stage method for generating certified stamp receipts for digital documents. The rejected claims include two independent claims – claims 29 and 41. Independent claim 29 is directed to the first stage, wherein a trusted outside agency generates an uncertified time stamp receipt and a message authentication code (MAC) for transmission to a requestor. Claim 41 is directed to the second stage, wherein the trusted outside agency certifies that time stamp receipt based on a valid MAC. Note that the claimed MAC is a one-way hash function that is generated at the outside agency based on the time stamp receipt and a secret key. Only the outside agency that generated the MAC (claim 29) has knowledge of that secret key, and thus, only that outside agency can verify the MAC. Therefore, only that agency can verify the time stamp receipt in the second stage of the claimed invention (claim 41).

Pasieka discloses various entities that create and digitally sign documents using an author's private key. These entities may be, for example, a network server or a notary. According to Pasieka, the entities generate successive hash values of a document and digitally sign each hash using their own secret key. Pasieka teaches that a given entity may hash a document that has already been cryptographically signed. However, this results only in “nested” cryptographic signatures. In Pasieka, the signing entities simply use their private keys to sign a hash result as is conventional. *Pasieka*, col. 4, ll. 49-57; col. 5, ll. 24-34. They do not employ their secret key as input into a one-way hash function.

This latter fact is plainly evidenced in Pasieka. Specifically, Pasieka teaches that other parties can validate the signed information so long as they have the published public key. *Pasieka*, col. 4, ln. 58 – col. 5, ln. 3; col. 6, ll. 1-9. Allowing other third parties to validate a

document contradicts the purpose of claimed MAC, where only the agency that generated the MAC can validate the MAC and certify the document.

The secondary reference, Schneier, does not remedy this deficiency and is utterly irrelevant to the claimed invention. Schneier merely introduces a general debate regarding public-key and symmetric cryptography. In fact, the Examiner fails to assert that Schneier stands for anything more. Schneier merely discusses that public-key and symmetric cryptography are different “sorts of animals” that solve “different sorts of problems.” *Schneier*, p. 216, §10.2. Nothing in Schneier relates to a MAC or to time stamp receipt generation or certification utilizing a MAC, and the Examiner does not assert that there is.

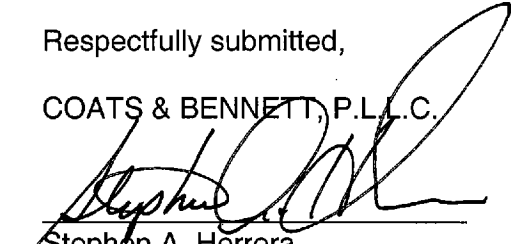
Therefore, it is confusing as to where the Examiner finds the alleged motivation to combine the references. Indeed, there is none. The Examiner simply alleges that because Schneier teaches that a symmetric (secret) key system is more beneficial than a public key system, one skilled in the art would be motivated to modify Pasioka to use a secret key rather than a public key. However, this statement regarding the Schneier teachings is inaccurate. Schneier actually teaches using different methods for different applications – not that one is more beneficial than the other. Further, because neither reference even approaches a discussion of a MAC, neither reference can support the motivation.

The cited references fail to teach or suggest, alone or in combination, any of claims 29-46 and 51-52. Therefore, the §103 rejection fails as a matter of law. Applicants respectfully

request the allowance of all pending claims.

Respectfully submitted,

COATS & BENNETT, P.L.L.C.



Stephen A. Herrera
Registration No.: 47,642

Dated: November 9, 2006

P.O. Box 5
Raleigh, NC 27602
Telephone: (919) 854-1844
Facsimile: (919) 854-2084